

09/914315

JC03 Rec'd PCT/PTO 24 AUG 2001

~~SECURED ACCESS DEVICE WITH CHIP CARD APPLICATIONS~~
BACKGROUND OF THE INVENTION

1.—

104230 31.6.60

SUBSTITUTE SPECIFICATION

SECURED ACCESS DEVICE WITH CHIP CARD APPLICATIONS

Field of the Invention

The present invention relates to a secured access device ~~with~~for chip card applications.

_____ More specifically, the invention relates to
5 a device for secured access to chip card applications
that uses ~~especially~~ instructions that have been
performed in the chip card which, at each instant,
provide information on rights, ~~especially in terms of~~
~~access to~~ for accessing the memory of the chip card,
10 the software component, or the hardware operation that
has been performed in the chip card.

_____ 2. _____

~~Description~~ Background of the Prior Art Invention

The most common type of chip card has a
15 microprocessor that manages a program memory. The
program memory is usually dedicated to a single
application or a set of applications loaded at the same
time into the chip card. When several applications are
loaded into a chip card, they have a close relationship
20 with one another, and are all designed for ~~one and~~ the
same type of service. Thus, for example, a chip card
cannot simultaneously play the role of a bank card and

09/914315-0000

that of a customer ~~loyalty~~ card for ~~another type of~~
business of any kind.

In order to end this situation where each
chip card has to be limited to one type of application,
5 new software architectures are being considered. These
new software architectures are making use of the
development of standardized programming languages ~~(for~~
~~example the language "JAVA")~~ which resolve the problems
of portability, such as the programming language JAVA,
10 for example.

Figure 1 is a simplified view of a software
architecture of the chip card ~~projects~~cards that are
now being developed. The architecture shown in Figure
1 ~~comprises~~includes, in particular, a first part 110
15 that corresponds to ~~what is called~~ the software
~~architecture of a chip card 100~~ and a second part 120
that corresponds to ~~what is called~~ the applications
part of the software architecture ~~offor~~ the chip card
100. The system part 110 ~~of the chip card~~ is
20 essentially formed by a library of programs 112 ~~offor~~
~~the chip card operating system of the chip card~~, an
interface 114 to manage the interactions with, ~~for~~
~~example,~~ the microprocessor ~~of the chip card or else~~or
the different memories of the chip card, and a space
25 for the management of hardware interruptions 116.

The applications part 120 of the software
architecture ~~consists of~~includes different
applications:

-----, such as a first, second and third main
30 application, respectively 122, 124 and 126;

-----, and a first, second and third additional
application, respectively 121, 123 and 125.

-----The main applications 122, 124 and 126 are
written in a programming language that can be directly
35 understood by the processor of the chip card.

00014315-002104
001200-512100

The additional applications 121, 123 and 125 are typically applications encoded in a standardized language. These applications may be added at any point in time to the system part 110 ~~in an applications part~~ 5 ~~120 of the software architecture described~~. In Figure 1, the additional applications 121, 123 and 125 depend directly on the first main application 122. The first main application 122 herein serves as an interpreter between the additional applications and the operating 10 system by converting the codes of the additional applications into a machine language that can be understood by the programs of the operating system 112.

~~_____ The device with secured access to applications of a chip card according to the invention comes into play in an architecture of this type.~~ 15

The software architecture that has just been described is more complex than the one currently existing in chip cards in circulation. ~~Indeed, t~~The architecture described assumes that it is possible to 20 add applications in a standardized programming language, possibly after the chip card is put into circulation. It is therefore more complicated to achieve a satisfactory level of security ~~than was the case~~compared to when a single application or a group of 25 applications dedicated to a single chip card function ~~was~~are the only applications to be loaded ~~once and for all~~ into the chip card ~~which~~. The chip card was then permanently limited in terms of available applications. The risk that a new application might disturb the 30 working operation of previous applications was therefore not as great.

The coexistence of applications of different kinds ~~in one and~~ the same chip card may raise a certain number of problems. For example, a software 35 architecture simultaneously containing an application

5

Summary of the Invention

10

15

25

35

program memory, and a battery of one or more
applications in a memory of the chip card, wherein t.

The device comprises:

_____ a register of the microprocessor to store a
5 code, on several check bits, proper to an entity
brought into play,

_____ . Also included are a call instruction, and
an instruction for the return of the set of
instructions to instantaneously and automatically
10 update the register during the action by a new entity.

_____. The device further includes a checking device for the checking, as a function of the check bits, ~~of the authorized character of the~~ whether access to the zones or address location of the memory of the chip card by the new entity that is called or comes into action in the chip card.

~~_____ a~~ is authorized. A first link ~~to transmits~~
the check bits from the microprocessor to the checking
device.

20 According to a particular embodiment of the device of the invention, each new entity ~~taking action~~being executed is activated at a predefined address of a ~~ROM (read only~~read only memory (ROM) ~~type memory~~ of the chip card.

25 According to different embodiments of the
invention, the entity ~~working~~operating in the chip card
may be an application of the ~~battery of~~one or more
applications or a hardware event, or ~~again~~ the
operating system associated with the microprocessor of
30 the chip card.

~~BRIEF DESCRIPTION OF THE DRAWINGS~~

Brief Description of the Drawings

The various aspects and advantages of the invention shall appear more clearly hereinafter in the following description made with reference to the

5 ~~Figure~~FIG. 1, ~~already described,~~ is a simplified ~~view~~block diagram of a software architecture ~~offor~~ for the chip ~~card projects~~cards currently being developed, according to the prior art; and

~~In Figure 2, a~~ according to the present invention. A microprocessor 200 ~~of a chip card 100~~ manages the set of operations ~~offor~~ for a ~~battery~~ plurality of applications 210 of the chip card 100.

Detailed Description of the Preferred Embodiments

For example, ~~when~~ an entity such as the application 211, ~~by means of a two-way bus 250~~ for
30 example, requires the intervention of another entity, such as an application 212, it sends a call instruction DCALL using the two-way bus 250 followed by a designation of the entity called and a parameter enabling the nature of the call to be determined.
35 According to the invention, a register R is updated

during such calls. A certain number of bits of the register R then assume a value associated with the called entity. The register R is therefore a hardware ~~means~~ component of the microprocessor 200 used to store
5 a code proper to the entity of the software architecture that is being performed, and to control its field of execution.

Furthermore, the device according to the invention may also take into account ~~of~~ instructions
10 known as hardware instructions, ~~for example such as~~ resetting type ~~instructions of the resetting type, for example.~~ Instructions known as hardware instructions are events that may occur in real time ~~on a chip card~~ and generate interruptions in the microprocessors of
15 the chip cards. This type of event is managed by the device ~~according to the invention~~ in the same way as the software instructions. ~~t~~ The bits of the register R take a very precise value, appropriate to each real-time event ~~that acts on~~ affecting the chip cards, thus
20 limiting and controlling the rights pertaining to these events.

The information given by the register R is thus capable of checking ~~a piece of information, for example at the microprocessor or any other entity~~
25 ~~external to the software architecture,~~ on the identification of the zone of the software architecture concerned by the application being executed. This information is checked at the microprocessor or at any other entity external to the software architecture.

30 The information given by the register R enables the checking of the zone of the memory of the chip card in which the application is ~~entitled to come into action, namely the memory space that it is~~ permitted to be accessed. Thus, any user attempting to
35 make fraudulent use of the operating system in order to

COPIES SENT

The addresses ~~which it is sought to be~~ accessed and the bits of the register R₇ sent by the microprocessor ~~by means of the~~ via link 230₇ are compared with each other in the access controller of ~~access to~~ the memory 220. Should it be the case that ~~If~~ the addresses of the memory ~~that it is sought to~~ to be accessed are not addresses belonging to the authorized field of the last application having performed a call instruction DCALL-type call, then ~~a piece of~~ information on illegal access ~~prohibits access to these~~ memories to the memory is prohibited.

_____A second register CS makes it possible to retain in memory a code proper to the applications that were active at the last call instruction DCALL sent by the current application, namely those that are to be performed following the current application.

The second register CS cannot be directly accessed by the applications of the chip card. This is
35 ~~in order~~ to ensure the integrity of the device when it

is put into operation during the execution of a return instruction DRET.

_____When the execution of the current application is finished, the bits of the register R
5 assume a value specific to the application that was being performed previously, restoring its rights and limits in terms of memory access.

_____The memory zone access device according to the invention gives a high level of security in terms
10 of access to the different zones of the memory, for a software architecture such as the one shown in Figure 1.

FOR SECRET

WHAT THAT WHICH IS CLAIMED IS--:

1. A device for access to applications of a chip card comprising a microprocessor associated with an operating system working with a set of instructions, a program memory and a battery of applications in a
5 memory of the chip card, wherein the device comprises:

—a register of the microprocessor to store a code, on several check bits, proper to an entity brought into play,

—a call instruction and an instruction for
10 the return of the set of instructions to instantaneously and automatically update the register during the action by a new entity,

—a checking device for the checking, as a function of the check bits, of the authorized nature of
15 the access to the zones of the memory of the chip card by the new entity that is called or takes action in the chip card,

—a first link to transmit the check bits from the microprocessor to the checking device.

2. A device for access to applications of a chip card according to claim 1, comprising a second register to store a code proper to the applications active at the time of the last call instruction sent.

3. A device for access to applications of a chip card according to one of the claims 1 or 2, wherein the entity that is called or takes action in the chip card is an application of the battery of
5 applications.

4. A device for access to applications of a chip card according to one of the claims 1 or 2, wherein the entity is a hardware event.

DocId:32876600

ABSTRACT OF THE DISCLOSURE

Disclosed is a

09445 STEH 60

SECURED ACCESS DEVICE WITH CHIP CARD APPLICATIONS

Abstract of the Disclosure

5 A device for secured access to applications
of a chip card, ~~bringing into operation~~ executes
instructions that provide information, ~~at each point in~~
10 ~~time, on the rights, especially in terms of access to~~
~~the chip card, of~~ on the rights for accessing the chip
card with respect to a software component or a hardware
action performed in the chip card. ~~In the case of~~ For
each new software component and at each new hardware
15 action, a register R of the microprocessor of the chip
card stores a specific code ~~that makes it possible to~~
~~check~~ for checking the authorized nature of the
operations ~~of access to the memory of the chip card~~
~~that are~~ performed by the new software component or
15 hardware action.

Figure 2

for accessing the memory of the chip card.

004431E 002104
401203 511100